

Міністерство освіти і науки України  
Тернопільський національний технічний університет  
імені Івана Пулюя

Кафедра  
комп'ютерних систем та мереж

**Методичні вказівки**  
для самостійної роботи студентів з дисципліни  
**Захист інформації у комп'ютерних  
системах**

спеціальність 123 “Комп'ютерна інженерія”

Тернопіль 2018 р.

Методичні вказівки для самостійної роботи студентів з дисципліни «Захист інформації у комп'ютерних системах» розроблені у відповідності з навчальним планом за спеціальністю 123 «Комп'ютерна інженерія»

УКЛАДАЧ:                      ст. викл. каф. КС Жаровський Р.О.

Методичні вказівки розглянуті і затвердженні на засіданні кафедри комп'ютерних систем та мереж, протокол №\_\_\_ від \_\_\_ \_\_ 2018 року.

Схвалено і рекомендовано до друку методичною комісією факультету комп'ютерно-інформаційних систем і програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя, протокол №\_\_\_ від \_\_\_ \_\_ 2018р .

## ЗМІСТ

Вступ.....	4
1 Тематичний план навчальної дисципліни «Захист інформації у комп'ютерних системах».....	8
2 Загальні рекомендації до організації самостійної роботи з дисципліни «Захист інформації у комп'ютерних системах».....	9
3 Вимоги до написання рефератів .....	13
4 Перелік тем для самостійного опрацювання.....	19
5 Система поточного й підсумкового контролю знань студентів .....	20
Список рекомендованої літератури .....	21

## ВСТУП

Методичні вказівки до самостійної роботи студентів з дисципліни «Захист інформації у комп'ютерних системах» розроблені відповідно до навчального плану та робочої програми дисципліни і призначені для студентів напрямку 123 “Комп'ютерна інженерія”

Метою викладання дисципліни є ознайомлення студентів зі способами захисту інформації у комп'ютерних системах. У курсі розглядаються основні підходи до розробки системи інформаційної безпеки комп'ютерних систем, сучасні апаратні і програмні засоби, призначені для захисту інформації, основні принципи функціонування систем захисту, що розроблені з використанням сучасних методів, технологій та засобів в середовищі електронно-обчислювальних систем і мереж з використанням знань, отриманих при вивченні окремих розділів вищої та прикладної математики, системного програмного забезпечення, систем керування базами даних, комп'ютерних мереж, програмування та інших дисциплін.

У результаті вивчення навчальної дисципліни «Захист інформації у комп'ютерних системах» *студент повинен здобути*

### **загальні компетентності:**

- Здатність застосовувати знання у практичних ситуаціях
- Здатність до адаптації та дії в новій ситуації
- Здатність оцінювати та забезпечувати якість виконуваних робіт
- Здатність до аналізу та синтезу
- Навички використання інформаційних і комунікаційних технологій
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел

### **фахові компетентності:**

- Ґрунтовна підготовка з математики для використання математичного апарату при розв'язанні прикладних і наукових завдань в області комп'ютерної інженерії
- Знання сучасних методів побудови та аналізу ефективних алгоритмів, основ теорії чисельних методів, і вміння їх реалізувати в конкретних застосуваннях
- Знання принципів програмування, засобів сучасних мов програмування, основних структур даних
- Знання загально-методологічних принципів побудови сучасних комп'ютерних систем з різною організацією для забезпечення високопродуктивної обробки інформації
- Знання принципів, методів та засобів проектування, побудови та обслуговування сучасних комп'ютерних мереж різного виду та призначення
- Знання організаційних, технічних, алгоритмічних і інших методів і засобів захисту інформації в комп'ютерних системах та мережах, відповідно законодавству та стандартам в цій області, з сучасними криптосистемами; вміння їх застосовувати в процесі професійної діяльності

#### **програмні результати навчання**

- Уміння застосовувати знання у практичних ситуаціях
- Уміння адаптуватись до нових ситуацій
- Уміння відповідально ставитись до виконуваної роботи та досягти поставленої мети
- Уміння застосовувати знання і розуміння для розв'язання задач синтезу та аналізу в системах, які характерні обраній спеціальності.
- Уміння використовувати інформаційні і комунікаційні технології для вирішення різних дослідницьких і професійних завдань
- Уміння здійснювати пошук інформації в різних джерелах для розв'язання задач спеціальності.

- Уміння застосовувати базові знання стандартів в області інформаційних технологій при розробці та впровадженні інформаційних систем і технологій
- Уміння застосовувати комп'ютерні засоби при проектуванні та створенні апаратних і програмних складових комп'ютерних систем та мереж
- Уміння опановувати та розробляти документацію на системи, продукти і сервіси інформаційних технологій, спілкуватись рідною мовою, професійно спілкуватись англійською мовою
- Вміти налаштовувати мережеві операційні системи
- Уміння використовувати засоби сучасних мови програмування для створення програмних продуктів, уміння їх застосовувати під час програмної реалізації алгоритмів професійних задач

**знати:**

- Основний склад і принципи функціонування систем захисту інформації;
- Принципи і методи криптографічного захисту інформації;
- Механізми і методи контролю КС;
- Принципи роботи основних типів шкідливих комп'ютерних програм і методи боротьби з ними.

**уміти:**

- Здійснювати захист інформації в КС або мережах;
- Розробляти та використовувати сучасні засоби та методи криптографічного захисту інформації;
- Виконувати розрахунки характеристик безпечного використання паролів та ключів шифрування;
- Виконувати проектування системи захисту інформації в КС та мережах, використовуючи сучасні засоби розмежування доступу користувача до критичної інформації з елементами аутентифікації суб'єктів та повідомлень;

- Адекватно обирати методи і засоби шифрування інформації;
- Виявляти і усувати потенційно небезпечні місця у системі безпеки комп'ютерних систем;
- Працювати з системним журналом і відслідковувати модифікацію системи.

Вивчення дисципліни «Захист інформації у комп'ютерних системах» передбачає засвоєння навчального матеріалу у вільний від аудиторних занять час у формі самостійної та індивідуальної навчально-дослідної роботи, призначеної формувати практичні навички роботи студентів із спеціальною літературою, орієнтувати їх на інтенсивну роботу, критичне осмислення здобутих знань і глибоке вивчення теоретичних і практичних проблем для підвищення якості професійної підготовки.

Самостійна робота над засвоєнням навчального матеріалу з дисципліни може виконуватися в бібліотеці, навчальних кабінетах та лабораторіях, в домашніх умовах. Згідно з навчальним планом дисципліни «Захист інформації у комп'ютерних системах» на самостійну роботу студентів відведено 87 годин.

Раціональна організація самостійної роботи вимагає від студента вмілого розподілу свого часу між аудиторною і позааудиторною роботою. Виконання завдань із самостійної та індивідуальної роботи є обов'язковим для кожного студента.

Методичні вказівки до самостійної роботи студентів включають:

- тематичний план навчальної дисципліни;
- загальні рекомендації до організації самостійної роботи з дисципліни, в тому числі до організації індивідуального наукового-дослідного завдання;
- систему поточного й підсумкового контролю знань студентів;
- список рекомендованої літератури.

Заключною формою самостійної роботи є підготовка до здачі модулів, заліку.

# **1 ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ»**

При вивченні дисципліни «Захист інформації у комп'ютерних системах» студент повинен ознайомитися з програмою навчальної дисципліни, її структурою, методами дослідження інформаційних систем, видами й методами контролю роботи комп'ютерних систем.

Тематичний план дисципліни «Захист інформації у комп'ютерних системах» складається з трьох модулів, які, в свою чергу, складаються із змістових модулів, кожен з яких об'єднує в собі відносно окремий самостійний блок дисципліни, що логічно пов'язує кілька укрупнених навчальних елементів дисципліни.

Навчальний процес здійснюється в таких формах: лекційні, лабораторні заняття і самостійна робота студента.



## **2 ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ДО ОРГАНІЗАЦІЇ САМОСТІЙНОЇ РОБОТИ З ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ У КОМП'ЮТЕРНИХ СИСТЕМАХ»**

Обов'язковим елементом успішного засвоєння навчального матеріалу дисципліни «Захист інформації у комп'ютерних системах» є самостійна робота студентів з вітчизняною і зарубіжною літературою з питань теорії, методології та практики проведення наукових досліджень за спеціальністю «Комп'ютерні системи та мережі»

Самостійна робота є основним засобом оволодіння навчальним матеріалом у час, вільний від нормованих навчальних занять, тобто лекційних, лабораторних і практичних занять (аудиторної роботи).

Основні види самостійної роботи, на які повинні звертати увагу студенти:

- вивчення лекційного матеріалу;
- робота з опрацювання та вивчення рекомендованої літератури;
- підготовка до лабораторних занять;
- робота над рефератом (тезами, доповіддю);
- робота над індивідуальним науково-дослідним завданням;
- підготуватися до дискусії в аудиторії щодо розуміння вивченого матеріалу;
- підготовка до поточного та підсумкового контролю.

*Опрацювання лекційного матеріалу.* У системі різних форм навчально-виховної роботи особливе місце належить лекції, де викладач надає студенту основну інформацію, навчає розмірковувати, аналізувати, допомагає опанувати ключові знання, а також спрямовує самостійну роботу студента.

Зв'язок лекції і самостійної роботи студента розглядається в таких напрямках:

- лекція як головна початкова ланка, що визначає зміст і обсяг самостійної роботи студента;

- методичні прийоми читання лекцій, що активізують самостійну роботу студентів;
- самостійна робота, яка сприяє поглибленому засвоєнню теми на базі прослуханої лекції.

Перший етап самостійної роботи починається з процесу слухання і записування лекції. Правильно складений конспект лекції – найефективніший засіб стимулювання подальшої самостійної роботи студентів. Складання і вивчення конспекту – перший етап самостійної роботи студента над вивченням теми чи розділу. Конспект допомагає в раціональній підготовці до практичних занять, заліку, у визначенні напрямку і обсягу подальшої роботи з літературними джерелами.

Таблиця 2.1 - Перелік тем лекцій і кількість годин для самостійної підготовки

№ з/п	Назва теми	Кількість годин	
		Денна форма навчання	Заочна форма навчання
1.	Основні поняття і аналіз загроз інформаційної безпеки	5	6
2.	Проблеми інформаційної безпеки мереж	6	6
3.	Політики безпеки	4	6
4.	Стандарти інформаційної безпеки	6	6
5.	Принципи криптографічного захисту інформації	4	8
6.	Криптографічні алгоритми	4	8
7.	Технології аутентифікації	6	6
8.	Забезпечення безпеки операційних систем	4	6
9.	Технології міжмережевих екранів	4	6
10.	Основи технології віртуальних захищених мереж VPN	4	7
11.	Захист на каналному і сеансовому рівнях	4	8
12.	Захист на мережевому рівні — протокол IPSEC	4	8
13.	Інфраструктура захисту на прикладному рівні	4	8
14.	Аналіз захищеності і виявлення атак	4	8
15.	Захист від вірусів	4	8
16.	Методи управління засобами мережевої безпеки	4	6
	<b>Разом</b>	<b>71</b>	<b>111</b>

Під час підготовки до лекції студент повинен опрацювати матеріал попередньої лекції з використанням підручників та інших джерел літератури. На лекціях висвітлюють тільки основні теоретичні положення та найбільш актуальні проблеми, тому більшість питань виноситься на самостійне опрацювання.

Викладач у вступній лекції рекомендує студентам основну і додаткову літературу, а також методичні рекомендації до самостійної роботи та до організації занять з дисципліни. У методичних вказівках з кожної теми наведено перелік питань для теоретичної підготовки до заняття.

У разі, коли студент не може самостійно розібратися в якомусь питанні, він може отримати консультацію у викладача (згідно з графіком проведення консультацій викладачами кафедри комп'ютерної інженерії). Добре організовані консультації дозволяють спрямувати самостійну роботу в потрібному напрямі, зробити раціональною і підвищити її ефективність.

*Підготовка до лабораторних занять.* Підготовка до лабораторних занять розпочинається з опрацювання лекційного матеріалу та теоретичних відомостей методичних вказівок до заданої роботи. Студент повинен самостійно ознайомитися з теоретичними відомостями, послідовністю виконання роботи та підготувати відповіді на контрольні запитання у певній послідовності згідно з логікою засвоєння навчального матеріалу.

Виконання лабораторних робіт збагачують і закріплюють теоретичні знання студентів, розвиваючи їх творчу активність, допомагають у набутті практичних навичок роботи.

У процесі підготовки до лабораторних робіт самостійна робота студентів є обов'язковою частиною навчальної роботи, без якої успішне і якісне засвоєння навчального матеріалу неможливе.

*Написання реферату дисципліни «Захист інформації у комп'ютерних системах»* (за темою курсового, дипломного проекту) є результатом роботи по кожній темі занять, які студент оформляє у вигляді реферату (відповідно до

методичних вказівок).

Роботу «Захист інформації у комп'ютерних системах» слід оформляти у відповідності до вимог, розроблених і затверджених профільною кафедрою. Обсяг - 12-15 друкованих сторінок.

### **3 ВИМОГИ ДО НАПИСАННЯ РЕФЕРАТІВ**

Дана робота складається з: титульної сторінки, змісту, вступу, основної частини, висновків, списку літератури, додатків.

Титульна сторінка повинна містити назву навчального закладу, кафедри, навчальної дисципліни; тему науково-дослідної роботи; прізвище та ініціали студента; номер академічної групи; дату подання роботи викладачеві на перевірку.

Зміст повинен містити назви розділів, підрозділів і т.д.), що розкривають тему роботи, із зазначенням номерів сторінок, на яких вони розміщені.

У вступі вказують актуальність обраної теми дослідження, її проблематику, об'єкт, предмет, мету і завдання дослідження.

Основна частина включає декілька розділів (підрозділів) і обов'язково складається з взаємопов'язаних теоретичної, аналітичної та рекомендаційної (практичної) частин.

У висновках викладають перелік пропозицій та рекомендацій та результати одержані в індивідуальній науково-дослідній роботі.

Реферат друкується або пишеться студентом на одній стороні аркуша паперу формату 210x297 мм. При цьому необхідно залишати поля: зліва – 25 мм, справа - 10 мм, поверх - 20 мм, знизу - 15 мм. Текст друкується на машинці або принтері через півтора проміжних інтервала, середня щільність друку - 30 рядків при 35-40 знаках у кожному рядку.

Текст реферату друкується розбірливо без виправлень. Помилки, описки і графічні неточності необхідно акуратно підчистити і написати полагоджений текст від руки чорнилом, пастою або тушшю. Ушкодження аркушів, виправлення не припускаються.

Виклад змісту реферату повинний бути стислим, чітким, що виключає можливість суб'єктивного тлумачення, і вестися від першої особи множинного числа, наприклад : "приймаємо", "вибираємо" і т.д. Мова викладення повинна бути технічно грамотною, не містити жаргонних виразів і маловживаних слів.

Варто користуватися єдиними і відповідними встановленими стандартом термінологією і визначеннями, а при їхній відсутності - загальноновживаними в науково-технічних джерелах.

Скорочення слів у тексті і підписах під ілюстраціями, як правило, не припускається.

Літерним позначенням різноманітних величин (значення символів і числових коефіцієнтів) при першому їхньому використанні варто давати розшифровування безпосередньо під формулою.

Розмірність того самого параметра в межах реферату повинна бути незмінною.

У записі обчислень по формулах, наводять тільки вихідну формулу, вираз із підставленими цифрами й остаточний результат. Проміжні розрахунки виключаються.

Весь текст реферату поділяють на розділи. Кожний розділ варто починати з нової сторінки. Розділи в межах реферату, а також підрозділи і пункти мають порядкові номери, позначені арабськими цифрами без крапки наприкінці, наприклад : 1 - перший розділ; 2 - другий розділ; 2.1 – перший підрозділ другого розділу; 2.1.1 - перший пункт першого підрозділу другого розділу. Вступ і висновок не нумеруються і виконуються великими літерами.

Заголовки розділів пишуть великими літерами посередині тексту. Заголовки підрозділів пишуть з абзацу, відступаючи зліва 15 мм, малими літерами (крім першої великої). У заголовку не допускаються переноси слів. Пропуски над заголовками і під ними - 2 см. Точку наприкінці заголовка не ставлять. Якщо заголовок складається з двох речень, тоді їх розділяють точкою. Заголовок підкреслювати не можна.

Нумерація сторінок повинна бути наскрізна. Номер сторінки проставляється арабськими цифрами в середині верхнього поля сторінки. На титульному аркуші число 1 не ставиться.

Текст реферату ілюструється схемами, графіками, таблицями. Всі ілюстрації іменуються рисунками, що нумеруються послідовно в межах розділу

арабськими цифрами. Номер рисунка повинен складатися з номера розділу і порядкового номера рисунка, розділених крапкою (наприклад, "Рис.2.5"- п'ятий рисунок другого розділу). Рисунки повинні бути чіткими і виконаними тільки чорними, синіми або фіолетовими чорнилами, пастою або тушшю, а також із використанням принтера. Кожний рисунок повинен супроводжуватися змістовним підписом. Підписи під рисунками або надписи над таблицями повинні бути стислими і пояснювати основний зміст. Підпис пишеться під рисунками в один рядок із номером.

Рекомендується весь матеріал, що пояснює рисунок, наводити в підрисунковому тексті, а не користуватися вільним місцем на рисунку. На всі ілюстрації повинні бути посилання в тексті. Посилання на раніше згадані ілюстрації і таблиці дають із скороченим словом “дивитися” (наприклад : “див. рис. 1”, -“див. табл. 1”).

Таблицю використовують для оформлення цифрового матеріалу та наводять після першого згадування про неї в тексті. На всі таблиці повинні бути посилання в тексті, при цьому слово “Таблиця” у тексті пишуть цілком, якщо таблиця не має номера, і скорочено, якщо має номер, наприклад: “...у табл. 1.2”. У повторних посиланнях на таблиці й ілюстрації варто вказувати скорочено слово “дивитися”, наприклад, “див. табл. 1.2”. Таблиці повинні нумеруватися в межах розділу арабськими цифрами. Над лівим верхнім кутом таблиці поміщають напис “Таблиця” із вказівкою порядкового номера таблиці. Номер таблиці складається з номера розділу і порядкового номера таблиці, розділених крапкою, наприклад: “Таблиця 2.4”- четверта таблиця другого розділу. Якщо в записах тільки одна таблиця, тоді її не нумерують.

Кожна таблиця повинна мати заголовок. Заголовок і слово "Таблиця" починають з великої літери. Заголовок не підкреслюють і виконують після слова “Таблиця” з номером таблиці через дефіс в тому самому рядку над таблицею. Заголовки граф таблиць повинні починатися з великих літер, підзаголовки - з маленьких, якщо вони складають одне речення з заголовком, і з великих, якщо вони самостійні. Робити заголовки таблиці по діагоналі не

дозволяється. Висота рядків повинна бути не менше 8 мм. Графу "№ п./п." у таблицю включати по можливості не слід.

Таблицю розміщують таким чином, щоб її можна було читати без повороту записки або з поворотом по годинниковій стрільці. При великій кількості рядків допускається перенесення таблиці на інший аркуш. При цьому заголовок поміщають тільки в її першій частині, над іншими частинами пишуть: “продовження таблиці\_\_\_” з вказівкою номера таблиці. Якщо повторюваний у графі таблиці текст складається з одного слова, його припускається замінити лапками; якщо з двох або більш слів, то при першому повторенні його замінюють словами “Те ж”, а далі - лапками.

Ставити лапки замість повторюваних цифр, знаків, марок, математичних символів не можна. Якщо цифрові або інші дані в якомусь рядку таблиці не наводять, тоді в ньому ставлять прочерк.

Формули в рефераті (якщо їх більш однієї) нумерують арабськими цифрами в межах розділу. Номер формули складається з номера розділу і порядкового номера формули в розділі, розділених крапкою. Номер ставиться з правого боку аркуша на рівні нижнього рядка формули в круглих дужках, наприклад: (3.1) - перша формула третього розділу. Посилання на формулу вказують порядковим номером формули в круглих дужках, наприклад, “... у формулі (2.1)”. Символи і числові коефіцієнти варто наводити безпосередньо під формулою, зі слова “де” без двокрапки після нього, в тій же послідовності, у якій вони подані у формулі.

Рівняння і формули варто виділяти з тексту вільними рядками. Якщо рівняння не поміщається в один рядок, воно повинно бути перенесене після знаків “ = ” або “ + ”, “ - ”, “ \* ”, “ : ”. Кожна формула, крім найбільш простих, повинна мати посилання на джерело, з якого вона взята, якщо вона не виводиться автором.

У перелік використаних джерел включають усі використані джерела в порядку появи посилань на них у тексті пояснювальної записки. При посиланні в тексті на використовувану літературу вказують порядковий номер, виділений



двома квадратними дужками за списком джерел, наприклад [20]. Джерело описується в наступній формі: прізвище та ініціали автора, повна назва книги або статті, місце і рік видання, обсяг (для часопису – назва часопису, рік видання, номер сторінки).

Приклад :

4. *Бусленко Н. П.* Моделирование сложных систем / Н. П. Бусленко. — М. : Наука, 1978. — 400 с.

Приклад посилання на статтю :

28. *Советов Б. Я.* Организация имитационных экспериментов в процессе обучения студентов специальности АСУ / Б. Я. Советов, А. В. Сочнев, С.А.Яковлев // В сб. : Применение ЭВМ в учебном процессе. — 1983. — С. 45-52.

Додатки оформляють як продовження реферату на наступних його сторінках або у вигляді окремої частини, розташовуючи їх у порядку появи посилань у тексті. Кожний додаток треба починати з нового аркуша. Додаток повинен мати заголовок, надрукований зверху маленькими літерами з першої великої симетрично відносно текста сторінки. Посередині рядка над заголовком маленькими літерами з першої великої повинно бути надруковано слово “Додаток\_\_\_” і велика літера, яка позначає додаток.

Додатки потрібно позначати послідовно великими літерами української абетки, за виключенням Г, Є, З, І, Ї, Й, О, Ч, Ї, наприклад, Додаток А, Додаток Б і т.д. Додатки повинні мати спільну з рештою записки наскрізну нумерацію сторінок, за винятком випадків, коли вони відносяться до різних видів документації.

Текст кожного додатка, при необхідності, може бути розділений на підрозділи, підрозділи, пункти і підпункти, що нумеруються арабськими цифрами в межах кожного додатка. Перед ними ставиться позначення додатка (літера) і крапка "А.2" – другий розділ додатка А; Г.3.1 – підрозділ 3.1 додатка Г; Д.4.1.2 – пункт 4.1.2 додатка Д; Ж.1.3.3.4 – підпункт 1.3.3.4 додатка Ж.

Рисунки, таблиці, формули нумерують в межах кожного додатка,

наприклад, рисунок Г.3 – третій рисунок додатка Г; таблиця А.2 – друга таблиця додатка А; формула (А.1) – перша формула додатка А.

Остаточно оформлений реферат підлягає доповіді в режимі співбесіди з викладачем. Для визначення рівня та якості засвоєння теоретичного і фактичного матеріалу приймаються такі вимоги:

- зміст реферату, його відповідність темі, повнота розкриття теми, логіка і послідовність написання тексту, самостійність думок, міркувань, суджень;
- використання, крім рекомендованої літератури, періодичних видань та інформації з мережі Internet;
- відповідність оформлення реферату вимогам нормативних документів;
- змістовність, логічність, лаконічність відповіді та відповідей на запитання, володіння матеріалом обраної теми.

#### 4 ПЕРЕЛІК ТЕМ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

№пп	Назва теми для самостійного опрацювання
1.	Захист системи від краху: резервне копіювання(UNIX, Windows). Системи аварійного відновлення. Резервне копіювання конфігурації системи і даних.
2.	Способи відновлення файлів і файлових систем при неумисному пошкодженні.
3.	Апаратні засоби аутентифікації у комп'ютерних системах(апаратні ключі, пластикові і smart-карти).
4.	Налаштування політик безпеки системного реєстру MS Windows.
5.	Динамічний моніторинг мережевих з'єднань, налаштування аудиту, робота з журналами безпеки в MS Windows.
6.	Динамічний моніторинг мережевих з'єднань, робота з системними журналами в UNIX-подібних операційних системах.
7.	Програмні засоби моніторингу вторгнень у комп'ютерну систему, цілісності і тестування комп'ютерної системи (SNORT, TRIPWIRE, OSEC, SATAN, SAINT, NMAP, NESSUS, HPING2 та ін.)
8.	Спеціалізовані програмні комплекси RTK і FRENZY.

## **5 СИСТЕМА ПОТОЧНОГО Й ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ СТУДЕНТІВ**

Оцінювання знань, вмінь і навичок студентів включає ті види занять, які згідно з програмою навчальної дисципліни «Дослідження і проектування комп'ютерних систем та мереж» передбачають лекційні, лабораторні, курсове проектування, самостійну роботу.

Перевірку і оцінювання знань студентів проводять в наступних формах:

- оцінювання виконання і захист лабораторних робіт;
- презентація результатів самостійної роботи;
- складання проміжного контролю знань за змістовими модулями;
- здача екзамену.

Для кожного змістовного модуля передбачено певну форму поточного контролю. Результати поточного контролю автоматично, без участі студента, зараховуються при модульному контролі. Студент може покращити результати поточного контролю при модульному контролі через тестування.

Передбачено підсумковий модульний контроль:

- залік.

Максимальна оцінка навчальної дисципліни - 100 балів.

## **СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ**

### **Базова**

1. Зегжда Д. П. Основы безопасности информационных систем. / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия —Телеком, 2000.
2. Лукацкий А. Обнаружение атак / А. Лукацкий. – СПб.: БХВ-Петербург, 2003.
3. Максим М. Безопасность беспроводных сетей / Пер. с англ. А. В. Семенова / М. Максим, Д. Полино. – М.: ДМ К Пресс, 2004.
4. Петров А. Компьютерная безопасность: криптографические методы защиты / А. А. Петров. – Москва: ДМК Пресс, 2000.

### **Допоміжна**

1. Галицкий А. В. Защита информации в сети — анализ технологий и синтез решений / А. В. Галицкий, С.Д. Рябко, В. Ф. Шаньгин - М.: ДМК Пресс, 2004.
2. Дшхунян В. Л. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты / В. Л. Дшхунян, В. Ф. Шаньгин - М.: АСТ: НТ Пресс, 2004.
3. ИСО/МЭК 14888-1—98. Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения.
4. ИСО/МЭК 14888-2—99. Информационная технология. Методы защиты. Цифровые подписи с приложением. Часть 2. Механизмы на основе подтверждения подлинности.
5. ИСО/МЭК 10118-1—94. Информационная технология. Методы защиты. Хэш-функции. Часть 1. Общие положения.
6. ИСО/МЭК 10118-2—94. Информационная технология. Методы защиты. Хэш-функции. Часть 2. Хэш-функции с использованием я-битного блочного алгоритма шифрации.
7. ISO 17799 — Международный стандарт безопасности информационных систем. 2002.
8. ISO/IEC 14443-1 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 1: Physical characteristics International Standard. 2000.
9. ISO/IEC 14443-2 Identification Cards — Contactless integrated circuit(s) cards Proximity Cards Part 2: Radio frequency power and signal interface International Standard. 2001.

### **Інформаційні ресурси**

1. Базовый стандарт организации беспроводных локальных сетей IEEE 802.11 [Електронний ресурс] / IEEE. – 1999. – Режим доступа до ресурсу: [http://standards.ieee.org/reading/ieee/std/lanman/802\\_11-1999.pdf](http://standards.ieee.org/reading/ieee/std/lanman/802_11-1999.pdf).

2. Беляев А. В. Методы и средства защиты информации [Электронный ресурс] / А. В. Беляев. – 2000. – Режим доступа до ресурсу: [http://www.citforum.ru/internet/infsecure/its2000\\_01.shtml](http://www.citforum.ru/internet/infsecure/its2000_01.shtml).
3. Коротыгин С. Развитие технологии беспроводных сетей: стандарт IEEE 802.11 [Электронный ресурс] / С. Коротыгин. – 2000. – Режим доступа до ресурсу: <http://www.ixbt.com/comm/wlan.shtml>.
4. Скородумов Б. И. Стандарты для безопасности электронной коммерции в сети Интернет [Электронный ресурс] / Б. И. Скородумов. – 2000. – Режим доступа до ресурсу: <http://www.stcarb.comcor.ru>.
5. Daemen J. Rijndael. Document version 2 [Электронный ресурс] / J. Daemen, V. Rijmen. – 1999. – Режим доступа до ресурсу: [www.esat.kuleuven.ac.be/~rijmen/rijndael](http://www.esat.kuleuven.ac.be/~rijmen/rijndael).